

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

FILED
UNITED STATES DISTRICT COURT
DENVER, COLORADO
10:56 am, Oct 22, 2021
JEFFREY P. COLWELL, CLERK

United States of America
v.
Paul Christian Welch

Case No. 2:21-mj-666
Colorado Case No. 1:21-mj-00175-KLM

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) Paul Christian Welch,
who is accused of an offense or violation based on the following document filed with the court:


☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☒ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

21 U.S.C. Section 841 - Knowingly or intentionally attempt to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense a controlled substance.

21 U.S.C Section 846 - Attempt and conspiracy to commit an act in violation of 21 U.S.C. Section 841.

Date: 10/13/2021


Chelsey M. Vascura
United States Magistrate Judge

Issuing officer's signature

City and state: Columbus, Ohio

Chelsey M. Vascura, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____

Arresting officer's signature

Printed name and title

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America

v.

Paul Christian Welch

Case No. 2:21-mj-666

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 2017 - June 2019 in the county of Franklin in the
Southern District of Ohio, the defendant(s) violated:

Code Section

Offense Description

21 U.S.C. § 841

Knowingly or intentionally attempt to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense a controlled substance.

21 U.S.C § 846

Attempt and conspriacy to commit an act in violation of 21 U.S.C. § 841.

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

Gregory Libow

Complainant's signature

Gregory Libow, Special Agent HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/13/2021

City and state: Columbus, Ohio

Chelsey M. Vascara

Chelsey M. Vascara
United States Magistrate Judge

Judge's signature

Chelsey M. Vascara, U.S. U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Gregory Libow, being duly sworn, state:

INTRODUCTION

1. I am a Special Agent with the HSI and have been since May of 2019. I am assigned to the Central Ohio Cyber Drug Taskforce (COCDTF) in Columbus, Ohio, where I am is responsible for conducting narcotics investigations involving dark web marketplaces. Prior to becoming a Special Agent, I was employed as a United States Customs and Border Protection (CBP) Officer for 8 years. While working for CBP, I was assigned to Columbus, Ohio and worked alongside HSI and other law enforcement agencies targeting drug and weapon shipments purchased off the internet. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Since working for HSI, I have been involved in narcotics-related arrests, executed search warrants that resulted in the seizure of narcotics, and participated in narcotics investigations. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate. In particular, I am aware that drug traffickers often operate on the Darknet to avoid detection by law enforcement.

2. I have participated in and conducted numerous investigations of violations of various state and federal criminal laws, including violations of Title 21 United States Code.

PURPOSE OF AFFIDAVIT

3. I am participating in an investigation concerning an organized group of known and unknown individuals who are suspected of involvement in criminal offenses against the United

States, namely, to manufacture, distribute or dispense a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. § 846.

4. The information set forth in this affidavit is based upon my knowledge, training, experience, and participation in investigations involving the smuggling, possession, distribution, and storage of narcotics and narcotics proceeds. This information is also based on the knowledge, training, experience, and investigations conducted by fellow law enforcement officers, who have reported to me either directly or indirectly. I believe this information to be true and reliable. I know according to the Federal Analogue Act, 21 U.S.C. § 813 any chemical substantially similar to a controlled substance listed in Schedule I or II of the Drug Enforcement Administration's (DEA) Controlled Substance Schedule is to be treated as if it were listed in Schedule I, if intended for human consumption. I know is it is a violation of 21 U.S.C. § 841 to manufacture, distribute or dispense a controlled substance and a violation of 21 U.S.C. § 846 to attempt or conspire to manufacture, distribute, or dispense a controlled substance.

5. The information contained in this affidavit is based upon my personal participation in this investigation, information obtained from other agents and detectives assisting in this investigation, and my review of records, documents, and other material relating to this investigation.

6. Because this affidavit is being submitted for the limited purpose of securing criminal complaints and arrest warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Brandon TVEDT, Paul WELCH, Michael FORT, Erick TYNDAL and Nicholas HOUSTON have violated 21 U.S.C. § 841 and 21 U.S.C. § 846.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The “dark web” is a portion of the “deep web”¹ of the Internet, where individuals must use an anonymizing software or application called a “darknet” to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the “clear web” or simply the “web”). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces (“DWM’s”), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM’s listed above, they also obtained images of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

b. “Vendors” are the dark web’s sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of “vendor accounts” on dark web marketplaces. Customers, meanwhile, operate “customer accounts.” Vendor and customer accounts are not identified by numbers, but rather monikers or “handles,” much like the

¹ The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as “trusted” vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency². Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. “Reshippers” are individuals working for, or with, darknet vendors who manage the reshipping of illegal substances to darknet customers. A reshipper’s location is typically chosen to maximize the efficiency of product distribution but may operate anywhere in the world. A reshipper will typically receive bulk drugs and packaging to addresses they control, repackage the drugs into specified amounts, and then mail the drugs to customers at locations and addresses specified by the darknet vendor for compensation

² Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

in fiat currency, crypto-currency, and/or drug product. A reshipper may have no direct communication with the vendor's customers or associate with the vendor's online presence. A reshipper acts much like a drop shipper: a form of business where a seller accepts customer orders but does not keep items on hand, and instead transfers the orders and the shipment details to either a manufacturer, or a fulfillment house which then ships the goods directly to the customer. I know from training and experience that darknet vendors utilize reshippers to distance themselves from their customers and minimize risks associated with darknet drug trafficking.

d. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

e. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.³ Cryptocurrency is not illegal in the United States.

f. Bitcoin⁴ (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.”

³ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

⁴ Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

An individual can “mine” bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

g. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key.”) A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the

holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

h. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of April 1, 2021, one bitcoin is worth approximately \$59,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

i. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR

code⁵ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

j. Bitcoin “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁶ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone

⁵ A QR code is a matrix barcode that is a machine-readable optical label.

⁶ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

8. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital

device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet

FACTS ESTABLISHING PROBABLE CAUSE
SUMMARY OF THE INVESTIGATION

9. On October 04, 2019, the Central Ohio Cyber Drug Taskforce (COCDTF) in Columbus, Ohio, consisting of investigators assigned to HSI, Drug Enforcement Administration (DEA), United States Postal Inspection Service (USPIS) and the Internal Revenue Service (IRS), executed a federal search warrant at a Columbus Target's residence, who was using an online moniker to purchase narcotics off the Darknet site Empire Market. Investigators found and seized computers, mobile phones, media storage devices, \$43,097.00 in U.S. currency, one 9mm pistol with a loaded magazine, controlled substances and miscellaneous documents from the residence. Analysis of the Columbus Target's mobile phone, along with his Darknet Empire Market account, indicated that he had been communicating with and purchasing liquid psychedelic mushrooms from an online vendor using the Darknet moniker "TRIPWITHSCIENCE" on a regular basis.

10. Open source research determined that "TRIPWITHSCIENCE" has operated on several Darknet markets since approximately 2014, totaling over 17,000 transactions: Empire Market (4,719 transactions), Agora (1,500 transactions), Apollon Market (47 transactions), Berlusconi Market (60 transactions), Cryptonia Market (199 transactions), Dream Market (6,400 transactions), Tochka Market (542 transactions), Hansa Market (567 transactions), Silk Road 2.0 (2,199 transactions) and Dark Market (823 transactions). The research also indicates that "TRIPWITHSCIENCE" may have operated on Nightmare Market, Andromeda Market, AlphaBay, Silk Road, Wall Street Market, Pandora, Black Market Reloaded, and numerous other

small Darknet markets, but the number of transactions associated with those markets is unknown.

11. “TRIPWITHSCIENCE” operated primarily on Monopoly, Televend and Cannahome Darknet marketplaces selling liquid psychedelic mushrooms in 9.0 milligram/gram vials for \$19.95 each. “TRIPWITHSCIENCE” specifically stated how to consume the controlled substance on his marketplace listings, verifying the controlled substance analogue was for human consumption.

12. From December 23, 2019 through November 20, 2020, HSI Columbus, with the assistance from DEA and USPIS, conducted twelve controlled liquid mushroom buys from “TRIPWITHSCIENCE” via Empire and Cannahome Markets. HSI Columbus purchased a total of approximately 545 grams of liquid psychedelic mushrooms during the twelve buys. HSI received and seized a U.S. Mail parcel associated with each buy containing suspected liquid psychedelic mushrooms. The Ohio Bureau of Criminal Investigation (BCI) Forensic Laboratory tested the contents of each parcel and determined them to be 4-Acetoxy-N,N-Dimethyltryptamine (4-AcO-DMT). This controlled substance is an analogue of 4-Hydroxy-N,N-Dimethyltryptamine (liquid psychedelic mushrooms), a schedule I controlled substance.

13. On or about October 22, 2020, HSI Columbus received data from a seized Darknet Marketplace that contained 34 Bitcoin withdrawal wallet addresses for “TRIPWITHSCIENCE’s” vender account. Using cryptocurrency analysis tracing, a Coinbase wallet was discovered sending and receiving Bitcoin from “TRIPWITHSCIENCE’s” withdrawal wallets. A subpoena was served to Coinbase for the subscriber information and account history associated with the Coinbase customer conducting the bitcoin transactions. Coinbase subpoena

returns revealed the user account, created on January 22, 2013, belonged to James Verl BARLOW.

14. While reviewing seized Darknet Marketplace data from “TRIPWITHSCIENCE,” HSI SAs discovered messages between “TRIPWITHSCIENCE and Darknet moniker “DARKLOIS.” The messages identified “DARKLOIS” as a shill account created by “TRIPWITHSCIENCE” to promote his business and create test shipments on his account. Agents discovered a similar conversation between “DARKLOIS” and Darknet vendor “PERFECTSHROOMS,” the only other account “DARKLOIS” reviewed and interacted with. HSI Special Agents identified two additional shill Darknet buyer accounts, “APPLETITS” and “BOTTLEWHISKEYSHL,” being used by “TRIPWITHSCIENCE” and “PERFECTSHROOMS” to promote their sales on multiple Darknet marketplaces including Hansa Market. “PERFECTSHROOMS” had listings on Televend, Monopoly and Cannahome marketplaces. The account had listings for 3.5 grams to 114 grams of “Organic Mushrooms” (*Psilocybe Cubensis* Shrooms) in capsule form. A February 14, 2020, Established Vender Application stated PerfectShrooms had processed 7,800 orders on 15 different darknet marketplaces.

15. An investigative search conducted on the darknet website Empire Market for the vendor “TRIPWITHSCIENCE” revealed a listing for “Liquid Mushrooms (Pure Psilocybin Extract).” The listing advertised vials of approximately 9mg of “Liquid Mushrooms” for \$19.95 each. The listing allowed buyers to purchase in unlimited quantities/increments. This search revealed “TRIPWITHSCIENCE,” who was active on the market from December 3, 2018, through November 23, 2019, had completed 2,555 transactions. There were 1,732 positive feedback

comments left for “TRIPWITHSCIENCE” during that time frame, which regularly commented on the quality of the product.

16. On November 30, 2020, HSI Special Agent Gregory Libow obtained a search warrant for the Google account of BARLOW, JIM.V.BARLOW@GMAIL.COM. Numerous items of evidentiary value were located including multiple spreadsheets referencing Darknet marketplaces and bitcoin transactions believed to be sales ledgers for “TRIPWITHSCIENCE” and “PERFECTSHROOMS.” In a spreadsheet titled “2015 TCS Accounting” were 9 tabs, 7 of the tabs were titled 2015 and contained known two letter abbreviations for darknet markets AlphaBay, Nucleus Market, Abraxas Market, MiddleEarth Marketplace, Evolution Market, Agora Market and Black Bank Market. A tab titled “2015 Received” appeared to list all 704 Darknet transactions from January 1, 2015 through December 9, 2015. A second spreadsheet titled “TCS Accounting.” showed tabs for each year from 2014 to 2021 and a summary tab. Each tab dated for a certain year showed a detail ledger. Many of the ledgers included references to Darknet marketplaces, bitcoin mixing services and drug transactions. The summary tab broke down each year’s net, average month, average day, and total bitcoins earned for the year. A third spreadsheet titled “TWS Sales Summation” was found by investigators on BARLOW’s Google Drive in a folder named “DNM,” known by law enforcement to be an abbreviation for Darknet Market. The spreadsheet showed a sales ledger for Liquid Mushrooms sold in July of 2014 on Silk Road, Agora and Evolution Darknet markets. The ledger claimed, at the time, the

TRIPWITHSCIENCE DTO was averaging 682 orders a month and selling approximately 2,555 vials per month.

17. On April 21, 2021, BARLOW and additional co-conspirators were arrested for warrants issued by the Southern District of Ohio for Conspiracy to Possess with Intent to Distribute Psychedelic Mushroom Analogue.

Brandon TVEDT AKA: FEANOR

18. During a search of BARLOW's computer seized on April 21, 2021, HSI Special Agent Libow obtained access to a hidden encrypted folder titled "SINK" that contained a large quantity of documents and records concerning the TRIPWITHSCIENCE DTO. A document saved as "4 Feanor7" in folder employee>payments>archived contained multiple items of evidentiary value detailing amounts of packages/vials shipped and transactions paid to FEANOR each month for their involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. The ledger represented payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to FEANOR from March 2018 through March 2020 and totaled \$139,158.70 in payments. The funds paid to FEANOR on the ledger included his salary and miscellaneous payments for vials, stamps, a "bottle cap dispenser", a VPN, USB drives, a scanner, and "liquid filler" used by FEANOR to further his/her drug trafficking for the DTO. The ledger specifically listed 4,140 packages, containing 32,591 vials of liquid mushrooms, mailed by FEANOR for the TRIPWITHSCIENCE DTO. Chemical analysis of the vials purchased during the investigation of TRIPWITHSCIENCE determined the vials each contained approximately 10.7 grams of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), the chemical structure of which is substantially similar to 4-Hydroxy-N,N-dimethyltryptamine (Psilocyn). Further, darknet listings for TRIPWITHSCIENCE indicated "Each 10ml vial = 2g dried shrooms = 9mg psilocybin". The

ledger is not believed to be all inclusive of all packages and vials shipped by FEANOR, nor orders FEANOR may have scraped from darknet markets to process orders for other drug shippers. The lab reported weight of approximately 10.7 grams of 4-AcO-DMT per vial multiplied by the 32,591 vials of “liquid mushrooms” reported on the ledger equaled approximately 345,723 grams of 4-AcO-DMT shipped by FEANOR and sold as “shrooms”. Special Agent Libow was able to review an additional spreadsheet located on BARLOW’s computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Special Agent Libow used the document to calculate the average kilograms per month the DTO sold. Special Agent Libow then determined the number of months each DTO member worked. Special Agent Libow multiplied the number of months worked by the kilograms per month sold by the DTO to determine the approximate number of kilograms each DTO member assisted the organization in distributing. Using this information, investigators were able to determine FEANOR worked approximately 25 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 1,061 kilograms of drugs trafficked.

19. In a word document titled “a address Shipper, Feanor (as of 2018-10-25) (lwt)” found in the employee folder contained address labels from Nutronics Nutrition in Salt Lake City, Utah to Brandon TVEDT at 11310 Grimes Avenue in Pearland, Texas 77584. The document also indicted the shipment was a Liquid and was sent from a Post Office at 1953 S 1100 E in Salt Lake City, Utah. Investigators know Genesis Nutronics was name of the company used by the TRIPWITHSCIENCE DTO to ship bulk quantity of liquid mushrooms found at other co-conspirator’s residences from the area of Salt Lake City, Utah. A U.S. Customs and Border Protection database query of 11310 Grimes Avenue revealed Brandon TVEDT received plastic

bottles matching the cargo description of bottles used by other TRIPWITHSCIENCE reshippers to package the liquid mushrooms for resale. These shipments include 129.2kgs of bottles on April 5, 2019, 26.50 kgs on July 12, 2018, 16.10 kgs on June 1, 2018, and a BC Northern Lights Hydro grow kit on March 9, 2012.

20. Found in BARLOW's SINK folder was a word document titled "4feanor7." The document contained transaction records, which appeared to be monthly funds paid to FEANOR during his involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs, and a job application-style questionnaire with answers provided by FEANOR. In the application FEANOR stated he was a 39-year-old male (born between 1978 and 1979) that was residing near Houston, Texas in the zip code of 77584 (Pearland, Texas). Additional statements found within the document indicated FEANOR resided with his elderly parents but in a detached structure on their property. Queries of open source databases showed a Brandon William TVEDT was born on July 1, 1979. A recent address associated with TVEDT is 11310 Grimes Ave, Pearland, Texas 77584. This address was also reflected on TVEDT's Texas DL information, which also lists Ron Tvedt and Kim Tvedt, suspected relatives, as emergency contacts. Open source information also indicated that the home is owned by Ronald Tvedt and Kimberly Tvedt and had a detached garage that appears to have a second level.

21. Blockchain analysis was conducted on the wallet addresses obtained from the encrypted hard drive / hidden folder "4 Feanor7" in folder employee>payments>archived on James BARLOW's computer, which was seized during BARLOW's arrest on April 21. This document represented crypto-currency payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to FEANOR from March 2018 through March 2020 for their involvement with the DTO. Analysis was able to determine FEANOR sent

payments received from the TRIPWITHSCIENCE DTO directly to Coinbase, Inc. Coinbase, Inc. was issued a subpoena for the Coinbase user associated with these transactions. Coinbase returns revealed these transactions were attributed to Coinbase user Brandon TVEDT and listed an address of 11310 Grimes Ave., Pearland, TX, 77584. This address is congruent with the address used by TVEDT to receive plastic bottles matching the cargo description of bottles used by other TRIPWITHSCIENCE reshippers to package the liquid mushrooms for resale.

Paul WELCH AKA: PACKMAN/PACHMANA

22. During a search of BARLOW's computer seized on April 21, 2021, HSI Special Agent Libow obtained access to a hidden encrypted folder titled "SINK" that contained a large quantity of documents and records concerning the TRIPWITHSCIENCE DTO. A document saved as "7 Packman" in folder employee>payments>archived. The "7 Packman" document contained multiple items of evidentiary value detailing amounts of packages/vials shipped and transactions paid to PACKMAN each month for their involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. The ledger represented payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to PACKMAN from June 2017 through June 2019 and totaled \$95,569.95 in payments. The funds paid to PACKMAN on the ledger included his salary and miscellaneous payments for "vials from China", "stamps", "printer", "liquid filler", and other supplies used by PACKMAN to further his drug trafficking for the DTO. The ledger specifically listed 2,747 packages, containing 22,183 vials of liquid mushrooms, mailed by PACKMAN for the TRIPWITHSCIENCE DTO. Chemical analysis of the vials purchased during the investigation of TRIPWITHSCIENCE determined the vials each contained approximately 10.7 grams of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), the chemical structure of which is substantially similar to 4-Hydroxy-N,N-dimethyltryptamine

(Psilocyn). Further, darknet listings for TRIPWITHSCIENCE indicated “Each 10ml vial = 2g dried shrooms = 9mg psilocybin”. The ledger is not believed to be all inclusive and is not believed to include all packages and vials shipped by PACKMAN. The lab reported weight of approximately 10.7 grams of 4-AcO-DMT per vial multiplied by the 22,183 vials of “liquid mushrooms” reported on the ledger equaled approximately 237,358 grams of 4-AcO-DMT shipped by PACKMAN and sold as “shrooms”. Special Agent Libow was able to review an additional spreadsheet located on BARLOW’s computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Special Agent Libow used the document to calculate the average kilograms per month the DTO sold. Special Agent Libow then determined the number of months each DTO member worked. Special Agent Libow multiplied the number of months worked by the kilograms per month sold by the DTO to determine the approximate number of kilograms each DTO member assisted the organization in distributing. Using this information, investigators were able to determine PACKMAN worked approximately 25 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 1,061 kilograms of drugs trafficked.

23. In a word document titled “zzold address Shippers, Packman (as of 20181108) (lwt)” was, what appeared to be, address labels from Nutronics Health in Sandy, Utah to Mary Welch at 44013 Gardner Drive in Alpharetta, Georgia 30009. The document also indicted the shipment was liquid and was sent from a Post Office at 8850 S 700 E in Sandy, Utah on April 20th. A U.S. Customs and Border Protection query of Mary Welch did not show her receiving any bottles similar to other known reshippers but a Paul WELCH living at 1205 Metropolitan Avenue SE Apt 319 in Atlanta, Georgia 30316, believed to be a relative of Mary Welch, received 7 shipments of the bottles between December 25, 2017, and March 26, 2019. The shipment on

December 25, 2017, to Paul WELCH is described as “plastic blue cap” which investigators know is the same color TRIPWITHSCIENCE specifically told his reshippers to buy. On April 06, 2019, WELCH received .52kgs of Mylar bags. Investigators know the PERFECTSHROOMS DTO used Mylar Bags to conceal the mushroom capsules sent to darknet customers.

24. Found in BARLOW’s SINK folder was a word document titled “7 Packman.” The document contained transaction records, which appeared to be monthly funds paid to PACKMAN during his involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs, and a job application-style questionnaire with answers provided by PACKMAN. At the time of the application, PACKMAN stated he was a 29-year-old male (born between 1987 and 1988), residing in Atlanta, Georgia in zip code 30307. Additionally, statements within this document indicated that PACKMAN had two sisters. Queries of open source databases showed a Paul Christian WELCH residing in Atlanta, Georgia was born on May 12, 1988. A recent address associated with WELCH was 1205 Metropolitan Ave SE Apt 333, Atlanta, Georgia. This address is reflected on WELCH’s DL. Possible family members identified for WELCH were Molly Welch; Maureen Welch; and Mary Welch.

25. A document titled “Addresses lwt.docx” found on an archived version of the SINK folder listed “Pachmana (a.k.a. Packman)” as having the following two addresses Paul Welch, 1261 Caroline ST NE, Apt 103 in Atlanta, Georgia 30307 and Paul Welch, 1205 Metropolitan Ave SE, Apt 319 in Atlanta, Georgia 30316.

26. Blockchain analysis was conducted on the bitcoin wallet addresses obtained from the encrypted hidden folder file “7 Packman” This document detailed cryptocurrency transactions for payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to PACKMAN from

June 2017 through June 2019 for his involvement with the DTO. Analysis was able to determine four transactions from a wallet cluster used by PACKMAN to Coinbase, Inc. Coinbase, Inc. was issued a subpoena for the Coinbase user associated with these transactions. Coinbase returns revealed these transactions were attributed to Coinbase user Paul Christian WELCH and listed two addresses for WELCH: 1261 Caroline Street Northeast, Apt 103, Atlanta, GA and 1205 Metropolitan Avenue Southeast, Apt. 319, Atlanta, GA. Both addresses are congruent with the documents saved by BARLOW concerning PACKMAN's location. Coinbase records showed bitcoin (BTC) transactions were received into WELCH's Coinbase account which matched multiple dates and amounts listed on the PACKMAN payment ledger. Blockchain analysis on WELCH's bitcoin addresses listed in the Coinbase subpoena return showed WELCH received BTC directly from PACKMAN's TRIPWITHSCIENCE/PERFECTSHROOMS payment addresses. Blockchain analysis further showed WELCH received BTC via one-hop transactions from PACKMAN payment addresses.

Michael FORT AKA: EXPLODICON

27. During a search of BARLOW's computer seized on April 21, 2021, HSI Special Agent Libow obtained access to a hidden encrypted folder titled "SINK" that contained a large quantity of documents and records concerning the TRIPWITHSCIENCE DTO. A document saved as "5 Explodicon" in folder employee>payments>archived contained multiple items of evidentiary value detailing amounts of packages/vials shipped and transactions paid to EXPLODICON each month for their involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. The ledger represented payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to EXPLODICON from March 2018 through February 2019 and totaled \$36,682.56 in payments. The funds paid to EXPLODICON on the ledger included his salary and miscellaneous payments

for vials, stamps, and “liquid filler” used by EXPLODICON to further his drug trafficking for the DTO. The ledger specifically listed 977 packages, containing 7,450 vials of liquid mushrooms, and a 1.3 gallon jug mailed by EXPLODICON for the TRIPWITHSCIENCE DTO. Chemical analysis of the vials purchased during the investigation of TRIPWITHSCIENCE determined the vials each contained approximately 10.7 grams of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), the chemical structure of which is substantially similar to 4-Hydroxy-N,N-dimethyltryptamine (Psilocyn). Further, darknet listings for TRIPWITHSCIENCE indicated “Each 10ml vial = 2g dried shrooms = 9mg psilocybin”. The ledger is not believed to be all inclusive of all packages and vials shipped by EXPLODICON, nor orders EXPLODICON may have scraped from darknet markets to process orders for other drug shippers. The lab reported weight of approximately 10.7 grams of 4-AcO-DMT per vial multiplied by the 7,450 vials of “liquid mushrooms” reported on the ledger equaled approximately 79,715 grams of 4-AcO-DMT shipped by EXPLODICON and sold as “shrooms”. Special Agent Libow was able to review an additional spreadsheet located on BARLOW’s computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Special Agent Libow used the document to calculate the average kilograms per month the DTO sold. Special Agent Libow then determined the number of months each DTO member worked. Special Agent Libow multiplied the number of months worked by the kilograms per month sold by the DTO to determine the approximate number of kilograms each DTO member assisted the organization in distributing. Using this information, investigators were able to determine

EXPLODICON worked approximately 11 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 467 kilograms of drugs trafficked.

28. In a word document title “Exploadicon trainvibe” was an application EXPLODICON filled out when applying for the TRIPWITHSCIENCE reshipper position. In the application EXPLODICON stated he was a 31-year-old male at the time of applying (born between 1985 and 1986) and lived in Charleston, South Carolina in a house with his girlfriend of two and one half (2.5) years. He also stated he went to school full-time and built lighting rigs for touring stage productions and weddings. EXPLODICON indicated his girlfriend was an esthetician.

Additional documents showed EXPLODICON worked for TRIPWITHSCIENCE from March 20, 2018 to February 01, 2019. HSI Columbus ran a query in the U.S. Customs and Border Protection (CBP) database using information from EXPLODICON’s application and identified Michael FORT at 10 Belvue Road in Charleston, South Carolina 29407 as a likely suspect. A CBP database query of international shipments showed Michael FORT received 8 shipments of bottles with a similar cargo description as other TRIPWITHSCIENCE reshippers between April 2018 and December 2018. Queries of open source databases showed Michael FORT in Charleston, South Carolina was born on July 2, 1986. A recent address associated with FORT is 10 Belvue Rd, Charleston, South Carolina. This address is also listed on FORT’s DL. A Facebook profile under the name Mikey Fort displayed a photo of an Asian male that matched the driver’s license photo of FORT. The Facebook profile indicated that FORT studied Audio Production at Full Sail University Online, studied Arts Management: Music Industry at College of Charleston, and is a Co-Owner/Designer at Holy City Lighting. His graduation date for Full Sail University is listed as 2021.

29. Blockchain analysis was conducted on the bitcoin wallet addresses obtained from the encrypted hidden file “5 Explodicon” in folder employee>payments>archived on James BARLOW’s computer. This document detailed cryptocurrency transactions for payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to EXPLODICON from March 2018 through February 2019 for his involvement with the DTO. Analysis was able to determine EXPLODICON sent payments received from the TRIPWITHSCIENCE DTO directly to Coinbase, Inc. Coinbase, Inc. was issued a subpoena for the Coinbase user associated with these transactions. Coinbase returns revealed these transactions were attributed to Coinbase user Michael Chad FORT and listed two addresses for FORT: 10 Belvue Road, Charleston, SC and 210 Calhoun Street, Apt A, Charleston, SC. This address is congruent with the address used by FORT to receive empty vials similar to those used by the TRIPWITHSCIENCE DTO. Coinbase records showed sixteen bitcoin (BTC) transactions were received into FORT’s Coinbase account, worth \$30,903 at the time of transaction, which were funded directly by EXPLODICON payment addresses. Blockchain analysis further showed additional one-hop transactions from EXPLODICON payment addresses and funds received from darknet markets and bitcoin mixing services.

Erick TYNDAL AKA: SHIPMAN

30. During a search of BARLOW’s computer seized on April 21, 2021, HSI Special Agent Libow obtained access to a hidden encrypted folder titled “SINK” that contained a large quantity of documents and records concerning the TRIPWITHSCIENCE DTO. Two spreadsheets titled “Accounting & Inventory 2014-2015” and “Accounting & Inventory 2016” included a ledger of total of vials being sent by each TRIPWITHSCIENCE reshipper biweekly. The spreadsheet indicated that SHIPMAN began reshipping vials for TRIPWITHSCIENCE on August 31, 2014

and stopped on July 16, 2016. During that time, the spreadsheet indicated that SHIPMAN shipped 15,604 vials. Chemical analysis of the vials purchased during the investigation of TRIPWITHSCIENCE determined the vials each contained approximately 10.7 grams of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), the chemical structure of which is substantially similar to 4-Hydroxy-N,N-dimethyltryptamine (Psilocyn). Further, darknet listings for TRIPWITHSCIENCE indicated “Each 10ml vial = 2g dried shrooms = 9mg psilocybin”. The ledger is not believed to be all inclusive of all packages and vials shipped by SHIPMAN, nor orders SHIPMAN may have scraped from darknet markets to process orders for other drug shippers. The lab reported weight of approximately 10.7 grams of 4-AcO-DMT per vial multiplied by the 15,604 vials of “liquid mushrooms” reported on the ledger equaled approximately 166,962 grams of 4-AcO-DMT shipped by SHIPMAN and sold as “shrooms”. Special Agent Libow was able to review an additional spreadsheet located on BARLOW’s computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Special Agent Libow used the document to calculate the average kilograms per month the DTO sold. Special Agent Libow then determined the number of months each DTO member worked. Special Agent Libow multiplied the number of months worked by the kilograms per month sold by the DTO to determine the approximate number of kilograms each DTO member assisted the organization in distributing. Using this information, investigators were able to determine SHIPMAN worked approximately 23 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 912.45 kilograms of drugs trafficked.

31. In BARLOW’s encrypted hidden SINK file was a word document titled “Addresses lwt.docx” that listed monikers along with names and addresses, believed to be used by DTO

“Ordermen” to ship the bulk drugs to the reshippers. In the document SHIPMAN was listed as Erick TYNDAL with an address of 145 Pierside Drive in Ormond Beach, Florida 32176. In between the name and address was a Facebook link for Erick Tynman of Ormond Beach’s Facebook page. A U.S. Customs and Border Protection database search revealed, between January 1, 2015 and June 9, 2016, Erick TYNDAL of 145 Pierside Drive in Ormond Beach, Florida received 7 shipments of bottles with a similar cargo description as other TRIPWITHSCIENCE reshippers. A public record search shows Erick TYNDAL (DOB: 10/09/1980) living at the address at the time of those shipments.

32. Blockchain analysis was conducted on a wallet address obtained from the encrypted hard drive / hidden folder “christmas email.odt” in folder employee>archived on James BARLOW’s computer, which was seized during BARLOW’s arrest on April 21. This document detailed an end of year bonus paid to SHIPMAN, BTC wallet address 1PT5fKiH1XcqsTbbgk9jR4UCcECEwmcM2u, in December of 2014 for their “hard work” for working for the TRIPWITHSCIENCE DTO. Blockchain analysis was able to determine a direct transaction from wallet address 1PT5fKiH1XcqsTbbgk9jR4UCcECEwmcM2u and an address at Coinbase, Inc. Coinbase, Inc. was issued a subpoena for the Coinbase user associated with this wallet address. Coinbase returns revealed the individual receiving these funds was attributed to Coinbase user Erick TYNDAL and listed an address of 145 Pierside Dr., Ormond Beach, FL, 32176. This address is congruent with the address TYNDAL received shipments of bottles matching the ones used by the TRIPWITHSCIENCE DTO. Blockchain analysis further showed

additional direct and/or one-hop transactions from TYNDAL's Coinbase account from darknet markets and bitcoin mixing services.

Nicholas HOUSTON AKA: DNA

33. During a search of BARLOW's computer seized on April 21, 2021, HSI Special Agent Libow obtained access to a hidden encrypted folder titled "SINK" that contained a large quantity of documents and records concerning the TRIPWITHSCIENCE DTO. Two spreadsheets titled "Accounting & Inventory 2014-2015" and "Accounting & Inventory 2016" included a ledger of total of vials being sent by each TRIPWITHSCIENCE reshipper biweekly. The spreadsheet indicated that DNA began reshipping vials for TRIPWITHSCIENCE on September 14, 2014 and was fired from the organization around March 9, 2015. During that time, the spreadsheet indicated that DNA shipped 2,781 vials. Chemical analysis of the vials purchased during the investigation of TRIPWITHSCIENCE determined the vials each contained approximately 10.7 grams of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), the chemical structure of which is substantially similar to 4-Hydroxy-N,N-dimethyltryptamine (Psilocyn). Further, darknet listings for TRIPWITHSCIENCE indicated "Each 10ml vial = 2g dried shrooms = 9mg psilocybin". The ledger is not believed to be all inclusive of all packages and vials shipped by DNA, nor orders DNA may have scraped from darknet markets to process orders for other drug shippers. The lab reported weight of approximately 10.7 grams of 4-AcO-DMT per vial multiplied by the 2,781 vials of "liquid mushrooms" reported on the ledger equaled approximately 29,756.7 grams of 4-AcO-DMT shipped by DNA and sold as "shrooms". Special Agent Libow was able to review an additional spreadsheet located on BARLOW's computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Special Agent Libow used the document to calculate the average kilograms per month the DTO sold.

Special Agent Libow then determined the number of months each DTO member worked. Special Agent Libow multiplied the number of months worked by the kilograms per month sold by the DTO to determine the approximate number of kilograms each DTO member assisted the organization in distributing. Using this information, investigators were able to determine DNA worked approximately 6 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 238 kilograms of drugs trafficked.

34. In BARLOW's encrypted hidden SINK file was a word document titled "Addresses lwt.docx" that listed monikers along with names and addresses, believed to be used by DTO "Ordermen" to ship the bulk drugs to the reshippers. In the document DNA was listed as Addison Houston with an address of 215 N Second Avenue, Unit N in Cleveland, Mississippi 38732.

35. Blockchain analysis was conducted on the wallet addresses obtained from the encrypted hard drive / hidden folder "DNA Firing" and "Notes- DNA" in folder employee>archived on James BARLOW's computer, which was seized during BARLOW's arrest on April 21. This document detailed crypto-currency transactions for payments from TRIPWITHSCIENCE to DNA from August 2014 to March 2015 for their involvement with the DTO. Analysis was able to determine DNA sent payments received from the TRIPWITHSCIENCE DTO directly to Coinbase, Inc. Coinbase, Inc. was issued a subpoena for the Coinbase user associated with these transactions. Coinbase returns revealed these transactions were attributed to Coinbase user Nicholas HOUSTON and listed an address of 215 N Second Ave. Apt. N., Cleveland, MS,

38732. This address is congruent with the address saved by BARLOW concerning DNA's location.

PROFFER STATEMENTS

36. On April 29, 2021, a proffer session with a cooperating defendant (herein referred to as CD1) was held. CD1 stated he/she posted ads in online forums to recruit "shippers" to work for the TRIPWITHSCIENCE DTO. Investigators know in the TRIPWITHSCIENCE DTO "shippers", also known as "reshippers", are individuals who receive bulk quantities of drugs from other members of the DTO and repackage the drugs into smaller quantities. The shippers are then sent regular ledgers, from other members of the DTO, indicating the customers names and addresses to mail these smaller quantities of drugs to. CD1 stated he/she also recruited his/her customers in the sale messages of his product. CD1 indicated he/she did not want to know the shipper's names and looked for individuals who lived in larger cities. CD1 stated he/she would test his/her shippers when they began shipping to see if they could complete orders properly. CD1 stated he/she had numerous shippers over the years including but not limited to: "SHIPMAN"; "DNA"; and "EXPLODICON", residing in Florida. CD1 stated he/she hired SHIPMAN to be a shipper around 2015 or 2016. CD1 stated SHIPMAN also went by "TINMAN" and believed his real name sounded similar to TINDALE or TINDELL. CD1 stated EXPLODICON was a shipper from 2017 until 2018 or 2019. CD1 stated he/she hired DNA and SHIPMAN but indicated he/she let DNA go quickly. CD1 stated shippers made approximately \$4,000 to \$5,000 per month or approximately \$90 to \$200 per day. CD1 stated he/she would

reimburse the cost of stamps plus \$4-5 a package for gloves and other expenses. CD1 also stated a shipper was paid \$2,000 per month salary and an additional \$1.40 per vial shipped.

37. On August 5, 2021, a proffer session with a second cooperating defendant (herein referred to as CD2) was held. CD2 stated after January of 2018 he/she and another co-conspirator received customers' order details and addresses from a third co-conspirator and would mix and ship the drugs in priority mail envelopes and stamps. CD2 stated he/she recalled shipping the priority mail envelopes with bulk drugs to addresses in Florida, North Carolina, and Texas. CD2 said he/she recognized the name Mary Welch. Investigators determined Mary Welch is the likely mother of Paul WELCH. Investigators believe WELCH was using the moniker FEANOR and having packages shipped to his mother in an attempt to obscure his identity.

38. On August 31, 2021, a proffer session with a second cooperating defendant (herein referred to as CD3) was held. CD3 told investigators that he/she recalled shipping bulk packages of 4-ACO-DMT concentrate to reshippers of the DTO, including but not limited to Brandon TVEDT, who utilized the moniker FEANOR, in Texas. CD3 indicated he/she recalled the moniker PACKMAN and the last name WELCH but gave no further details.

CONCLUSION

39. Based on the foregoing facts, I believe that there is probable cause that Brandon TVEDT, Paul WELCH, Michael FORT, Erick TYNDAL and Nicholas Houston attempted and conspired to manufacture, distribute, or dispense a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. §846.

40. Accordingly, I request the issuance of a criminal complaint and arrest warrant for Brandon TVEDT, Paul WELCH, Michael FORT, Erick TYNDAL and Nicholas HOUSTON.

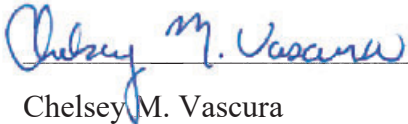
I further request that due to the ongoing nature of this investigation, the application, search warrant, and this affidavit be sealed until further ordered of the Court in order to avoid premature disclosure of the fact of this investigation and the information contained in this affidavit.



Special Agent Gregory Libow

Homeland Security Investigations

Subscribed and sworn to before me this 13th day of October, 2021.



Chelsey M. Vascara

United States Magistrate Judge